REMARKS/ARGUMENTS

Claims 1-5 stand rejected under 35 U.S.C. § 112, second paragraph as being indefinite. Claim 1 was deemed to lack clear antecedent basis language respecting the terms "interval key," "interval index" and "system." By amendment to claim 1, each of the terms have amended or articles of speech have been modified to establish clear antecedent basis. No new matter has been added by the claims, and the scope of the claims have been unchanged by these amendments.

Claims 1-5 stand rejected under 35 U.S.C. §103(a) over the Bao reference, also out of Singapore, which was published less than one year prior to the filing date of the subject application. Bao has been cited for containing teaching of all aspects of the invention except the use of an escrow agent that generates both public and private keys to all users, whereas the Young reference teaches use of an escrow agent or trusted party to generate public keys for all users.

As to Claim 2, Bao has been cited for disclosing that the parties exchange interval indexes.

As to claim 3, the Examiner takes notice of the common practice of discarding keys.

As to claims 4 and 5, Bao is cited for teaching that the interval index and the starting interval key are not communicated to the escrow agent.

The Applicant respectfully traverses this rejection. Neither Bao standing alone, nor Bao in view of Young, teaches the use of a key generation system that allows the parties to continue secure communication even after the trusted key generator or escrow agent has been compromised and after all secrets of the trusted key generator have become known to the attacker. The present invention teaches the use of public key-private key pairs for use in encryption key updating. The protection of secrecy after the key generator has been compromised is an important distinction in the operation of this invention.

By contrast to the present invention, any compromise of the key generator in Bao extinguishes the protection afforded to secret communications among parties. Bao teaches a system wherein messages are segmented and then communicated as (short) sequences with an

iteratively updated key which by its nature could be subject to compromise by an attacker having access to the initial message and the interim messages. Bao specifically teaches the sharing of a secret key with the decrypting party (Bao, pages 3 and 4: each method mentioned in the summaries includes a step of accepting a shared cryptographic (secret) key), which of course means that if the communication link is compromised or the key generator is compromised, and such information falls into the hands of an attacker, the attacker can reconstruct messages using these secret keys.

In the present invention, the reconstruction of the message using the public key is rendered highly improbable, because the actual message that is communicated does not employ the public key or even its own computation of the private key to communicate the encrypted message. Rather, the public key and private key are used to generate a further interval key pair that is used in exchange with other nodes in the communication system to communicate the message. Thus the attacker would not likely be able to decode the message, even from a complete record of the communication of all parties, *since the transmission is encrypted with an interval key that communicates the second public key that has been encrypted with the first public key*, and thus the attacker would not have access to the entire communication before its keys are destroyed. This is a nested generation and communication of public cryptographic keys independent of the escrow agent. The communications and key computations can be performed with further nestings to provide even greater security.

In the present invention, the successive interval keys are derived by encrypting the current interval key with a public key, and then replacing the current interval key with the encrypted result. This defines a sequence of interval keys k_1, k_2, ...,k_n where--at any one time--only one interval key is stored in the trusted key generator. Only an index on the interval keys needs to tracked, so each party may know which interval key is to be used for the then-current session. Notably, earlier generations of the keys have been destroyed (e.g., as in claim 3).

Consider the situation when the trusted key generator is compromised. The attacker may for example retrieve an interval key k_m. The attacker does *not* obtain the private key because the private key is not stored in the trusted key generator. Now note that earlier messages are encrypted with interval keys k_l where $l < m$. With no loss of generality, assume l =

$m-1$. To derive k_{m-1}, the attacker would have to decrypt k_m without knowledge of the private key. Put another way, if the attacker were able to derive k_{m-1} from k_m, then the method used by the attacker can be employed as an oracle or subroutine to perform decryption without the private key. This is widely regarded as cryptographically very difficult.

To emphasize this distinction, claim 1 has been amended to recite "causing said escrow agent to communicate only said first public key to all parties within a communication system ..." and " wherein only said starting interval key is encrypted by said first public key ...," thereby clearly distinguishing over Bao. While there may be other ways to state the aforementioned distinctions or to incorporate the aforementioned limitations into claims, it is believed that the amended claim limitations are sufficient for present purposes.

As to claims 2, it is noted that Bao accepts a shared secret key and the shared initial value as inputs, and it sets an index to an initial value. In the present invention, claim 2 recites specifically the computation of a next key for use in encryption (i.e., the second public key), as part of the nesting process.

Claim 3 calls for the discarding of the older interval key. While this may sound like a familiar process, the environment of the claimed invention would suggest that the key be retained and not be discarded. Step 210 in Bao even suggests that there is evidently no provision that would permit the discarding of a key. Hence, this claim represents a non-obvious departure.

As to claims 4 and 5 the Examiner has assumed that there is no communication with the escrow agent, but in fact, the Bao methodology and system rely on updates from the escrow agent in the course of the message (Step 210), so there is evidently continuing communication at some level with the escrow agent.

In view of the foregoing arguments and clarifying amendments, it is respectfully submitted that the claimed invention represents a patentable advance in the art represented by Bao.

The Examiner is thanked for the citation of references. The references have been reviewed and are deemed to be no more relevant than the applied references.

CONCLUSION

In view of the foregoing, the Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

Kenneth R. Allen

Kenneth R. Allen
Reg. No. 27,301

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (650) 326-2400
Fax: (650) 326-2422

Attachments
KRA:deh

60352864 v1